

REMARKS**1. Claim Rejections under 35 U.S.C. 101:**

5 Claims 1-27 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. In claims 1, 11, 20 and 25 (and by dependency the associated dependent claims), the first and second stations comprise the various elements as recited in the claim language including "a [first/second] hyperframe number (HFN)...". A number per se is non-statutory subject matter.

10

Response:

1.1 **Regarding claim 1:** In an effort to overcome the rejections under 35 U.S.C. 101, as set forth on page 2 of the above detailed office action, claim 1 is amended by
15 removal of direct references to a first hyperframe number and a second hyperframe number, references remaining where the above numbers are used in the system, for example in the amended claim 1:

20 "a decryption unit capable of decrypting received PDUs according to at least a first ciphering key, a first m-bit hyper frame number (HFN) which is a function of the FN for each received PDU, and the FN of each received PDU;"

and

25 "an encryption unit capable of encrypting transmitted PDUs according to at least the first ciphering key, a second m-bit HFN which is a function of the FN for each transmitted PDU, and an FN associated with each transmitted PDU;"

30 The hyper frame numbers now simply being recited as number stored in the system, for example in the medium access control (MAC) layers (129 & 139) of Fig.8, should not be considered non-statutory matter.

In addition, "capable of assigning each transmitted PDU with an n-bit FN" is

added to clarify that the FN of the transmitted PDU is assigned by the second station.

1.2 **Regarding Claim 11:** In an effort to overcome the rejections under 35 U.S.C. 101, as set forth on page 2 of the above detailed office action, claim 11 is amended by clarification of the language used to recite the relationship of hyperframe numbers to the device where it may previously not have been clear that the hyperframe numbers, each being associated with a PDU, are data used by the receiving buffer and extraction unit, and are not recited as device elements. A description of this relationship can be found in the specification between page 19, line 10 and page 20, line 22, and page 21, line 21 and page 22, line 11, (inclusive) respectively.

The amended claim 11, like the amended claim 1 now reciting the hyperframe numbers as numbers stored in the system, should therefore not be considered as containing non-statutory matter.

In addition, a first ciphering key and a second ciphering key are also amended to be recited as numbers stored in the system.

1.3 **Regarding Claims 20-24:** These claims are hereby canceled.

1.4 **Regarding Claim 25:** In an effort to overcome the rejections under 35 U.S.C. 101, as set forth on page 2 of the above detailed office action, claim 25 is amended by the removal of the recitation of "a first m-bit hyperframe number (HFN)" as a device element in the preamble, together with its associated method step. Claim 25 is amended instead to recite the HFN as data used by the subsequent method steps. Support for amendments to the first and second steps:

"the first station placing an identifying FN for identifying a layer 2 protocol data unit (PDU) in a stream of PDUs, into a first field of a message;"

"the first station placing x least significant bits (LSBs) from a first m-bit hyper frame number (HFN) value associated with the identifying FN in a second field of the message, the HFN being incremented by a first value upon detection of roll-over of an FN in the stream of PDUs; and"

can be found in the specification between page 19, line31 and page 20, line 22 (inclusive).

Support for amendments to the forth step:

5 “the second station receiving the message and using the x LSBs of the second field to determine a cyclical position of the identifying FN of the first field.”

can be found in the specification between page 19, line31 and page 21, line 19 (inclusive).

10 The amended claim 25, like the above amended claims now reciting the hyperframe numbers as numbers stored in the system, should therefore not be considered as containing non-statutory matter. Consideration of amended claims 1, 11, 20 & 25 is politely requested. No new matter is introduced by the above amendments.

15 **2. Claim Rejections under 35 U.S.C. 102:**

Claims 1-27 are rejected under 35 U.S.C. 102(b) as being anticipated by Finkelstein et al, U.S. Patent 5,319,712.

20 Although both the present invention and the cited prior art relate to synchronized layer 2 ciphering schemes for packetized data, the Applicant finds the cited art (Finkelstein et al. U.S. Patent 5,319,712, hereinafter referred to as Finkelstein) to be directed toward synchronized ciphering of packetized data with a fixed session key within one communication session [Finkelstein, col. 3, lines 34-41]. Whereas, the
25 claimed invention is directed toward ensuring that data packets are decrypted using the correct cipher key, at and around the time of a cipher key change. With regard to the cipher key issue, which in the present invention can change many times within one connection session, Finkelstein refers only to the use of a session key, this preferably being a shared secret data (SSD) key derived from a previous completed
30 authentication process by the communication units, i.e. the cipher key or the session key is decided at communication session startup [Finkelstein, col. 3, lines 34-41]. Finkelstein discloses that an exchange of acknowledge messages at call startup and

following handoffs may be required in order to unambiguously initialize the overflow counters [Finkelstein, col. 4, lines 59-62]. However, this is only done at call startup and handoff according to the teachings of Finkelstein. The Applicant finds the cited art vague regarding the particular issue of mid-session cipher key changes.

5

2.1 Regarding claim 1; "A method for synchronizing a ciphering key change in a wireless communications system comprising: a first station capable of receiving a security mode command...the second station determining an activation time at which a ciphering key change is to occur;"

10

Response:

The Examiner indicates that the above section of claim 1 of the instant invention is anticipated by Finkelstein (col. 1, lines 52-64, col. 2, lines 4-13, and col.3, lines 20-58). The Applicant points out that Finkelstein does not supply details of how to handle cipher key changeovers within one connection session, other than providing a method for establishing ciphering at session startup or handoff. In particular, the ciphering scheme taught by Finkelstein must always be started with the same session key from the first PDU up to the last PDU transported between the communication units. However, there are situations where a mid-session cipher key change may be required. Examples include: arrangements whereby a particular cipher key, under the auspices of a predetermined security protocol for example, has a finite validity in terms of real time (or in the 'application time' sense), hence a key change is required after a predetermined time period elapses during a connection session, or after the processing of a predetermined number of PDUs as appropriate; or, instances wherein the connection session is commenced without data ciphering being implemented, ciphering subsequently being selected during the session (or deselected in a reversal of the above situation), effectively forcing establishment of a ciphering key 'on-the-fly'.

30

The method recited in the amended claim 1 of the present invention is directed at cipher key changeover and will allow the above mentioned situations,

whereas Finkelstein does not teach a method with such capabilities.

- 2.2 Continuing with claim 1: "the second station composing the security mode command, the security mode command comprising a switching FN
5 corresponding to the activation time, and x least-significant bits (LSBs) from the second HFN corresponding to the activation time;"

Response:

- 10 The Examiner indicates that the above section of claim 1 of the instant invention is anticipated by Finkelstein (col. 3, line 59 to col. 4, lines 32). As discussed in section 2.1 above, Finkelstein's invention does not teach a method with ciphering key changes. Thus, no activation time on a particular switching FN (or sequence number in Finkelstein's terminology) is alluded to by
15 Finkelstein.

- 2.3 Continuing with claim 1: "the first station receiving the security mode command; the first station utilizing the switching FN and the x LSBs from the second HFN contained in the security mode command to obtain an application
20 time;"

Response:

- 25 The Examiner indicates that the above section of claim 1 of the instant invention is anticipated by Finkelstein (col. 4, line 48 – col. 5, line 33). As discussed in sections 2.1 and 2.2 above, Finkelstein's invention does not teach a method with ciphering key changes. Again, no application time is alluded to by Finkelstein.

- 30 2.4 Continuing with claim 1: "the first station using the first ciphering key to decrypt PDUs with FNs sequentially prior to the application time, and using a second ciphering key to decrypt PDUs with FNs sequentially on or after the

application time.”

Response:

- 5 The Examiner indicates that the above section of claim 1 of the instant invention is anticipated by Finkelstein (col. 1, line 65 – col. 2, line 14, col. 5, lines 33-65). As discussed in section 2.1 above, Finkelstein and the prior art disclosure of same only introduce ciphering as a general requirement for secure communications and discuss encoding and decoding using a common cipher key
- 10 by establishing said key at session startup, changes of cipher key at other times is not discussed or taught. The amended claim 1 emphasizes the change of ciphering keys by explicitly stating that the second ciphering key is different from the first ciphering key.
- 15 2.5 **Regarding claims 2-10:** Claims 2-10, being dependent upon the amended claim 1, should be allowed if the amended claim 1 is considered allowable.
- 2.6 **Regarding claim 11:** Claim 11 was rejected for the same reasons as claim 1. The amended claim 11 should be allowed if the amended claim 1 is considered
- 20 allowable.
- 2.7 **Regarding claims 12-19:** Claims 12-19, being dependent upon the amended claim 11, should be allowed if the amended claim 11 is considered allowable.
- 25 2.8 **Regarding claim 25:** “A method for removing cyclical ambiguity of an n-bit identifying frame number (FN) transmitted in a signaling message from a first station to a second station ... and the first station transmitting the message to the second station;”

30 Response:

The Examiner indicates that the above section of claim 25 of the instant

invention is anticipated by Finkelstein (col. 1, lines 52-64, col. 2, lines 4-13, col. 3, lines 20-58, col. 3, line 59-col. 4, line 32), however, the Applicant points out that the cited art does not teach the use of "x least significant bits" where $x < m$. To better recite a key feature of the claimed invention, i.e. the ability to provide unambiguous identification of PDUs using partial HFNs, an additional limitation, "wherein $x < m$ ", is included in the amended claim 25, x referring to the LSBs of a HFN and m being the bit-length of the HFN. Support for this amendment can be found in the specification on page 17, line 22, and page 19, line 13, wherein the respective preferred embodiment values for x and m are recited.

2.9 Continuing with claim 25: "wherein after reception of the message, the second station uses the x LSBs of the second field to determine a cyclical position of the identifying FN."

Response:

The Examiner indicates that the above section of claim 1 of the instant invention is anticipated by Finkelstein (col. 1, line 65-col. 2, lines 14, col. 4, line 48-col. 5, line 65), however, as with section 2.10 above, the Applicant points out that, the cited art does not teach the use of "x least significant bits" where $x < m$.

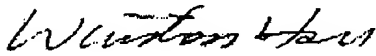
2.10 Regarding claims 26-27: The amended Claim 27 clarifies how the second HFN is maintained by the second station to keep the second HFN synchronized with the first HFN, and is amended by the inclusion of "the second HFN being incremented by the first value upon detection of roll-over of an FN in the stream of received PDUs". Support for this amendment can be found in the specification between page 19, line 31 and page 20, line 15 (inclusive), particularly page 20, lines 6-7. Claims 26, 27, being dependent upon the amended claim 25, should be allowed if the amended claim 25 is considered allowable.

2.11 Regarding claims 28-29: New claims 28, 29, being dependent upon the amended claim 1, should be allowed if the amended claim 1 is considered allowable.

5 2.12 Regarding claims 30-31: New claims 30, 31, being dependent upon the amended claim 11, should be allowed if the amended claim 11 is considered allowable.

10 In summary, the Applicant asserts that the claimed invention is capable of synchronizing multiple cipher key changes in a communication system while utilizing partial HFNs, whereas the cited art (Finkelstein) does not teach similar capabilities. Reconsideration of claims 1-19, 25-31 in light of the above discussion is politely requested. No new matter is introduced by the above amendments.

15 Sincerely,



Date: JUL 23 2004

20 Winston Hsu, Patent Agent No. 41,526
P.O. BOX 506
Merrifield, VA 22116
U.S.A.

e-mail : winstonhsu@naipo.com.tw

25 (Please contact me by e-mail if you need a telephone communication and I will return your call promptly.)